ICS 35.040
CCS L 80

MH

中华人民共和国民用航空行业标准

MH/T XXXXX—XXXX

民用航空重要网络和信息系统商用密码应用要求

Commercial cryptography application requirements for critical cyber and information system of civil aviation

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国民用航空局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国民用航空局综合司提出。

本文件由中国民航科学技术研究院归口。

本文件起草单位：中国航空油料集团有限公司、中国民航信息网络股份有限公司、河南省机场集团有限公司、中国民用航空西南地区空中交通管理局、中国民用航空总局第二研究所、中国国际航空股份有限公司、北京海泰方圆科技股份有限公司、中电科网络安全科技股份有限公司、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、国家商用密码应用技术研究工程中心等。

本文件主要起草人：夏伟、李绪国、周子站、李辛阳、苏力行、项熙艳、王欣、张韶华、宁文冠、龚丽、郭睿、翟冬梅、罗影、焦亨炼、黄晶晶、张晓娜、王亮、张东海、陈彦平等。

民用航空重要网络和信息系统商用密码应用要求

1 范围

本文件规定了民用航空重要网络和信息系统商用密码应用的基本要求、增强要求、扩展要求、产品应用要求及商用密码应用安全性评估要求。

本文件适用于中华人民共和国境内民用航空领域网络安全保护等级为第三级及以上的网络和信息系统（含关键信息基础设施）的商用密码应用规划、建设、运行、测评和监管等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022 信息安全技术 术语

GB/T 37092—2018 信息安全技术 密码模块安全要求

GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求

GM/T 0133—2024 关键信息基础设施密码应用要求

3 术语和定义

GB/T 25069—2022、GB/T 39786—2021界定的以及下列术语和定义适用于本文件。

3.1

民用航空重要网络和信息系统 critical cyber and information system of civil aviation

民用航空有关单位使用和维护的网络安全保护等级第三级及以上的网络和信息系统（含关键信息基础设施）。

3.2

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源：GB/T 39204—2022, 3.1]

3.3

空中交通管理类信息系统 air traffic management information system

对空中交通管制信息、航空气象信息以及航行情报信息进行收集、加工、处理和发布的信息系统。

注：包括空中交通管制自动化系统、民航气象信息系统、航行通告自动化处理系统、自动转报系统、空中交通流量管理系统、中小机场空管业务系统等。

3.4

航空器运行保障类信息系统 aircraft operational service information system

支撑指挥和操纵航空器飞行、开展适航维修等业务的信息系统。

注：包括航班运行控制系统、机务维修管理系统、电子飞行包系统、航材管理系统、机组服务保障系统等。

3.5

航空服务类信息系统 aviation service information system

提供客运、货运等航空运输服务和通用航空服务的信息系统。

注：包括航班座位控制系统、离港控制系统、代理人分销系统、电子客票系统、常旅客管理系统、货运管理系统、通用航空管理系统等。

3.6

机场生产运行类信息系统 airport operation information system

以航空业务保障为核心的机场信息系统。

注：包括信息集成系统、航班信息显示系统、广播系统、行李处理系统等。

3.7

航空安全保卫类信息系统　aviation security information system

提供安全检查、物理访问控制、安全监控等功能的信息系统。

注：包括安全检查信息管理系统、飞行区围界安全防范系统、门禁系统、机场控制区的通行证件管理系统、视频监控系统等。

3.8

行业监管与企业安全管理类信息系统　industry regulation and corporate safety management information system

支持各级民用航空政务部门开展安全监管和市场监管以及企事业单位开展安全管理的信息系统。

注：包括民用航空飞行标准监督管理系统、民用航空行业监管执法系统、航线航班管理系统、航班时刻管理系统、航空安全管理系统等。

3.9

公共信息服务类信息系统　public service information system

面向公众提供信息发布、信息查询、文化娱乐、广告宣传等服务的信息系统。

注：包括门户网站系统以及移动应用程序（不含订票、值机等业务应用）、文娱及商业信息发布系统等。

3.10

通用管理类信息系统　general management information system

以办公自动化为核心的实现企业资源管理的信息系统。

注：包括办公自动化系统、财务管理系统、电子邮件系统、视频会议系统等。

3.11

基础支撑类设施平台　foundational infrastructure and platform

多个民用航空信息系统在计算、操作、存储、通信、安全等方面所依赖的网络设施及信息系统。

注：包括通信网络设施、云计算平台、大数据平台、物联网平台、业务中台、数据中台、统一身份认证系统、网络安全监测防护平台等。

3.12

其他信息设施　additional information system

工业控制系统以及新型民用航空信息设施。

注：包括机场助航灯光监控系统、机场供油控制系统、智慧民航相关新型信息系统等。

3.13

密码算法　cryptographic algorithm

描述密码处理过程的算法。

[来源：GB/T 25069—2022, 3.380]

3.14

机密性　confidentiality

采用密码技术保证信息不泄露的性质。

[来源：GB/T 25069—2022, 3.259]

3.15

真实性　authenticity

一个实体是其所声称实体的性质。

[来源：GB/T 25069—2022, 3.769]

3.16

数据完整性　data integrity

数据所具有的特性，即无论数据形式作何变化，数据的准确性和一致性均保持不变。

[来源：GB/T 5271.8—2001, 08.01.07]

3.17

不可否认性　non-repudiation

也称抗抵赖性，证明一个已经发生的操作行为无法否认的性质。

[来源：GB/T 25069—2022, 3.321]

3.18

身份鉴别　identity authentication

证实一个实体所声称身份的过程。

[来源：GB/T 39786—2021，3.8]

3.19

旁路模式　bypass mode

当商用密码产品发生故障时，为保障业务不中断自动切换至非密码保护状态以保障业务连续运行的机制。

4　缩略语

下列缩略语适用于本文件。

PLC：可编程逻辑控制器（Programmable Logic Controller）

RTU：远程终端单元（Remote Terminal Unit）

SSL：安全套接层（Secure Socket Layer）

5　总则

5.1　商用密码应用保护对象

采用商用密码技术保护的民用航空重要网络和信息系统中有关业务数据、配置数据、操作行为和实体身份等。典型保护对象或应用场景示例见附录A。

5.2　商用密码应用强度

5.2.1　网络安全保护第三级及以上的网络和信息系统、相应保护等级的关键信息基础设施，应满足第6章规定的基本要求。

5.2.2　网络安全保护第四级及以上的网络和信息系统、相应保护等级的关键信息基础设施，应满足第6章和第7章规定的基本要求、增强要求。

5.2.3　关键信息基础设施在满足5.2.1或5.2.2所列相应要求的基础上，应同时满足第8章规定的扩展要求。

6　商用密码应用基本要求

6.1　物理和环境安全

6.1.1　宜采用密码技术对进入重要物理区域（如重要机房等）的人员进行身份鉴别。

6.1.2　宜采用密码技术保护电子门禁系统进出记录的存储完整性，留存期限不少于6个月。

6.1.3　宜采用密码技术保护视频监控音像记录数据的存储完整性，留存期限不少于3个月。

6.2　网络和通信安全

6.2.1　应采用密码技术对系统、设备的服务端、客户端等通信实体进行身份鉴别，保护通信实体身份的真实性。

6.2.2　应采用密码技术建立安全通信通道，宜支持密钥动态协商更新。

6.2.3　宜采用密码技术保护通信过程中数据的完整性。

6.2.4　应采用密码技术保护通信过程中重要数据的机密性。

6.2.5　宜采用密码技术保护网络边界的访问控制列表等访问控制信息的完整性。

6.2.6　可对移动智能终端、工业控制设备、物联网终端等外部接入设备采用密码技术进行接入认证。

6.3　设备和计算安全

6.3.1　应采用数字证书认证、动态口令认证等密码技术对登录服务器、数据库、网络设备、安全设备、密码设备等设备的用户进行身份鉴别，保护用户身份的真实性。

6.3.2 远程管理设备时，应采用密码技术建立安全的信息传输通道，不应明文传输操作指令。
6.3.3 宜采用密码技术保护用户身份鉴别信息传输和存储过程中的机密性。
6.3.4 宜采用密码技术保护系统资源访问控制信息、重要信息资源安全标记的完整性。
6.3.5 宜采用密码技术保护设备登录、远程管理和操作、审计管理等日志记录数据完整性。
6.3.6 宜采用密码技术校验设备固件、核心应用程序的完整性并验证来源真实性。

6.4 应用和数据安全

6.4.1 应采用密码技术对通过客户端程序、浏览器、受理终端、应用程序接口等方式登录或访问应用系统的用户进行身份鉴别。
6.4.2 宜采用密码技术保护信息系统应用的访问控制信息的存储完整性。
6.4.3 宜采用密码技术保护重要业务信息资源的安全标记（如数据分类分级、安全敏感等级、业务关键程度、合规性管理等）的完整性、真实性、一致性与可验证性。
6.4.4 应采用密码技术保护重要数据传输和存储过程中的机密性。
6.4.5 宜采用密码技术保护重要数据传输和存储过程中的完整性。
6.4.6 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，保护数据原发行为和接收行为的不可否认性。

6.5 管理制度

6.5.1 应建立覆盖人员、密钥、建设运行、应急处置、密码产品及软硬件介质等密码应用安全管理制度体系，并与现有网络和数据安全管理制度体系相衔接。
6.5.2 应根据密码应用方案，制定根密钥、对称密钥、非对称密钥等密钥的全生命周期管理规则，明确密钥产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节的操作流程与安全要求。
6.5.3 应针对密钥管理、密码设备操作等有关岗位人员，制定日常管理、设备运维、应急处置等操作规程，明确操作权限、流程及责任追溯要求。
6.5.4 应根据需要对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订完善并正式发布实施，修订周期每 3 年不少于 1 次。
6.5.5 应妥善留存设备巡检记录、配置核查记录、密钥生命周期管理记录等操作规程执行记录，留存期限不少于 1 年。

6.6 人员管理

6.6.1 应设置密钥管理员、密码操作员、密码安全审计员等关键岗位，建立密码应用岗位责任制度，明确各岗位职责与权限，关键岗位实行多人共管。密码安全审计员不应兼任密钥管理员、密码操作员。
6.6.2 密钥管理员、密码安全审计员、密码操作员等关键岗位人员应由本单位内部员工担任，上岗前应对其安全背景进行调查，签订保密协议，明确保密义务。
6.6.3 应对关键岗位人员每年至少开展 1 次密码安全专项培训和考核，内容涵盖法律法规、制度流程、技术操作、密码应用、应急处置等，考核合格方可上岗或继续任职，培训和考核记录留存时间不少于 3 年。
6.6.4 关键岗位人员离岗时，应终止其密码应用相关的所有访问权限、操作权限，收回智能密码钥匙、动态令牌等相应密码产品和设备，保存并及时更新资产台账。
6.6.5 应对相关设备与系统的管理账号、动态令牌、个人数字证书实行一人一号管理。

6.7 建设运行

6.7.1 新建、改造升级重要网络和信息系统时，应在规划设计阶段编制密码应用方案，经商用密码应用安全性评估机构评估通过后作为实施依据。
6.7.2 根据密码应用方案确定系统涉及的密钥种类、密钥体系架构及其全生命周期各环节的管理要求，密钥管理应符合本文件中 6.9 的规定。
6.7.3 应根据通过评审的密码应用方案制定密码应用实施方案，并根据密码应用实施方案开展系统建设，保护密码技术、产品与系统集成的一致性、有效性。
6.7.4 系统投入运行前应委托商用密码应用安全性评估机构开展商用密码应用安全性评估，评估通过后正式上线运行。

6.7.5 应每年委托商用密码应用安全性评估机构开展商用密码应用安全性评估，根据评估结果制定整改方案并进行整改，整改记录留存时间应不少于3年。
6.7.6 当系统发生重大变更（如密码方案调整、核心设备替换、业务范围变更等）时，应重新修订商用密码应用方案并委托商用密码应用安全性评估机构进行评估，通过评估后实施变更。变更完成后应重新对系统开展商用密码应用安全性评估，评估通过后上线运行。
6.7.7 应定期开展攻防对抗演习，明确攻防对抗演习具体内容，包括但不限于分析识别密码应用脆弱性，开展验证或模拟攻击和防御，明确攻防对抗演习组织形式、进度安排、资源保障等。针对密码应用攻防对抗演习中发现的问题，应及时进行整改。

注：密码应用脆弱性包括但不限于密码功能被旁路、密码产品和服务错误配置、用户非法操作导致的问题等。

6.8 应急处置

6.8.1 应制定密码应用安全应急预案，明确应急响应流程、责任主体、处置措施及资源保障，覆盖密钥泄露、密钥丢失、密码设备故障、密码服务中断、密钥管理系统异常等场景。应急处置措施应不影响核心业务连续性。
6.8.2 发生密码应用安全事件后，应立即启动应急预案、采取止损措施（如冻结密钥、切换备用设备）并向行业主管部门报告。事件处置完成后，应及时向行业主管部门及归属的密码管理部门提交完整的事件处置报告，内容包括事件原因、影响范围、处置措施、整改方案及责任认定等。应结合事件处置情况及时修订和完善密码应用应急预案。
6.8.3 应每年对系统相关人员进行密码应用应急处置培训，并每年至少组织1次应急演练，演练内容包括预案启动、故障处置、业务恢复等。演练结束后开展总结评估，应根据评估结果优化应急预案，演练记录与评估报告留存应不少于3年。
6.8.4 应储备密码设备、应急密钥（离线存储）、技术支持团队等必要的应急资源。

6.9 密钥管理

6.9.1 密钥生成

6.9.1.1 应在符合GB/T 37092—2018安全要求的密码模块内生成密钥，密钥生成过程应具备满足安全要求的熵值和不可预测性。
6.9.1.2 不应人工生成、设置弱密钥、固定密钥。

6.9.2 密钥分发

6.9.2.1 宜通过加密安全通道分发密钥，不应通过明文传输密钥，保护分发密钥的机密性和完整性。
6.9.2.2 密钥分发过程中，应对收发双方进行双向身份鉴别，保护身份的真实性。
6.9.2.3 会话密钥应采用一次一密机制。

6.9.3 密钥导入、导出

6.9.3.1 密钥的导入、导出应执行严格的授权审批流程，仅授权人员在指定场景下操作。
6.9.3.2 密钥导入时应校验密钥的完整性、真实性和格式合规性，校验通过后生效。
6.9.3.3 密钥导出时应采用加密封装形式，不应采用明文方式导出除公钥以外的密钥。
6.9.3.4 应对密钥导入、导出的过程进行记录，采用密码技术保护操作日志的完整性。

6.9.4 密钥存储

6.9.4.1 根密钥、主密钥应存储于专用硬件密码模块或合规密钥管理系统中。
6.9.4.2 工作密钥应加密后存储。
6.9.4.3 应对根密钥采取逻辑（物理）隔离存储。
6.9.4.4 可明文形式存储公钥，但应采取措施防范非授权篡改。

6.9.5 密钥使用

6.9.5.1 应遵循最小权限、按需授权原则使用密钥，仅允许授权主体按审批流程调用对应密钥。
6.9.5.2 不同业务应用、类型和级别的数据宜使用独立的密钥，不应复用跨业务、跨安全级别的密钥。
6.9.5.3 密钥明文不应出现在通用中央处理器（CPU）、内存、磁盘等密码模块外部非安全区域。

6.9.5.4　公钥在分发、使用过程中不应被非授权修改和替换，不应非授权访问、使用、泄露、修改和替换除公钥外的其他密钥。
6.9.5.5　应采用数字签名等密码技术保护操作行为不可否认性。
6.9.5.6　在密钥超过使用期限、已泄露或存在泄露风险时，应根据相应的更新策略进行更新。
6.9.5.7　应把密钥的调用纳入重要操作审计范围。

6.9.6　密钥备份与恢复

6.9.6.1　应制定规范的密钥备份与恢复流程。
6.9.6.2　备份介质应异地、离线存放，与生产环境物理隔离，并定期校验备份数据的可用性。
6.9.6.3　密钥恢复应执行严格的授权审批流程，恢复完成后应立即验证密钥的有效性和业务适配性。

6.9.7　密钥归档与销毁

6.9.7.1　对于已过期但因业务审计、数据追溯等需求留存的密钥，应执行归档管理。
6.9.7.2　归档密钥应存储在离线安全介质中，明确归档期限且不低于对应业务数据的法定留存期限。
6.9.7.3　归档密钥的访问应执行严格的授权审批，不应非授权访问归档密钥。
6.9.7.4　公钥证书应建立撤销机制，证书到期后应自动撤销，当密钥泄露、人员离职、设备报废等情况发生时，应立即启动密钥撤销流程。
6.9.7.5　过期、废弃、泄露的密钥应采用安全方式彻底销毁，硬件存储介质中的密钥应采用物理销毁方式，逻辑存储的密钥应采用符合国家密码标准的加密擦除方式。
6.9.7.6　密钥销毁应执行授权审批流程，2 人及以上在场监督操作，全程留存审计记录，销毁完成后进行验证。

6.10　安全审计

6.10.1　应将数据解密、身份鉴别、访问控制、密钥管理等相关操作纳入重要业务操作范围进行审计，审计日志覆盖操作主体、操作时间、操作内容、操作结果等核心要素。
6.10.2　宜对审计日志采用密码技术保障传输和存储过程中完整性，防止被篡改。
6.10.3　审计日志留存期限应不少于 6 个月。

7　商用密码应用增强要求

7.1　物理和环境安全

7.1.1　应采用密码技术对进入重要物理区域（如重要机房等）的人员进行身份鉴别，访问权限变更经过授权审批，宜采用基于生物特征等双因子认证机制。
7.1.2　应采用密码技术保护电子门禁系统进出记录的存储完整性，留存期限不少于 6 个月。
7.1.3　应采用密码技术保护视频监控音像记录数据的存储完整性，留存期限不少于 3 个月。

7.2　网络和通信安全

7.2.1　应采用密码技术对通信实体进行双向身份鉴别，保护通信实体身份的真实性。
7.2.2　应采用密码技术保护通信过程中数据的完整性。
7.2.3　应采用密码技术保护网络边界访问控制信息（如访问控制列表、防火墙策略、路由配置等）的完整性，防止非授权篡改。
7.2.4　宜采用密码技术对从外部连接到内部网络的设备进行接入认证，保护接入设备身份的真实性。

7.3　设备和计算安全

7.3.1　应采用密码技术对登录服务器、数据库、网络设备、安全设备、密码设备等设备的用户进行身份鉴别，保护用户身份的真实性。
7.3.2　应采用密码技术保护系统资源访问控制信息、设备权限配置信息的完整性。
7.3.3　应采用密码技术保护设备中的重要信息资源安全标记的完整性，防止安全标记被篡改。
7.3.4　应采用密码技术保护身份鉴别、远程管理和操作、审计管理等日志记录数据的完整性。
7.3.5　应采用密码技术保护重要可执行程序（如可执行程序、执行依赖程序、涉及软件或固件远程更

新的程序等）和版本信息的完整性和来源的真实性。

7.4 应用和数据安全

7.4.1 应采用密码技术保护重要操作行为（含重要业务操作、重要用户操作或异常用户操作等）的访问控制信息和操作行为记录的完整性。
7.4.2 应采用含密码技术的多因素身份鉴别机制，结合数字证书、生物特征识别、任务授权，使操作人员身份与任务匹配。
7.4.3 应采用密码技术保护信息系统应用的重要信息资源安全标记的完整性。
7.4.4 在可能涉及法律责任认定的应用中，应采用密码技术实现重要操作行为的不可否认性，实现数据原发行为的不可否认性和数据接收行为的不可否认性。

7.5 管理制度

应按照密钥保护数据的重要性制定差异化管理制度，对保护重要业务数据和个人敏感信息的密钥采用额外增强管理措施。

7.6 人员管理

关键岗位人员应签订长期保密协议，离职后保密义务存续期应不少于2年。

7.7 建设运行

7.7.1 应按照商用密码应用方案进行建设，密码产品和服务应与各种应用系统正确、合规、有效集成，对密码应用建设活动的质量、进度、文档和变更工作进行监督控制和科学管理。
7.7.2 当密码应用被转移、终止或废弃时，应采取安全可靠的方法转移、暂存和清除密钥等数据，迁移或废弃密码产品，清除或销毁相关存储介质。

7.8 应急处置

发生密码应用安全事件后，应及时向行业主管部门及属地密码管理部门报告。

7.9 安全审计

7.9.1 应每半年开展 1 次关键操作与密钥管理专项审计，形成审计报告，发现异常情况立即启动核查与处置流程。
7.9.2 审计日志留存期限应不少于 1 年。

8 关键信息基础设施商用密码应用扩展要求

8.1 网络和通信安全

8.1.1 关键信息基础设施边界内各等级保护对象之间，以及边界内与边界外等级保护对象之间进行网络通信时，应采用密码技术对通信双方实体（含设备、应用系统等）进行身份鉴别，未授权实体不应接入。
8.1.2 关键信息基础设施边界内各等级保护对象之间，以及边界内与边界外等级保护对象之间进行网络通信时，应采用密码技术保护通信过程中数据的机密性和完整性。

8.2 设备和计算安全

8.2.1 对密码产品和服务进行运维管理时，应形成对重要运维操作的日志，使用密码技术保护日志记录的完整性。
8.2.2 应采用密码技术保护重要可执行程序（如可执行程序、执行依赖程序、涉及软件或固件远程更新的程序等）和版本信息的完整性和来源的真实性。
8.2.3 宜对 PLC 控制器、RTU 等工业控制设备的程序下载、固件升级使用数字签名验证来源真实性和完整性。
8.2.4 如设备不支持上述功能，应采用工业控制安全隔离网关或密码机进行指令级的完整性校验和边界拦截等风险缓解措施。

8.3 应用和数据安全

8.3.1 应采用密码技术验证采集的核心数据、重要数据和敏感个人信息的来源真实性。
8.3.2 应采用密码技术保护核心数据、重要数据和敏感个人信息及其备份数据在传输（含边界内流动、跨边界流动、通过网络隔离产品流动）和存储过程中的机密性和完整性。
8.3.3 应严格管理核心数据解密功能的操作权限，将数据解密操作纳入重要业务操作范围进行审计。

8.4 管理制度

应制定密码产品全生命周期管理制度，明确密码产品采购、验收、升级、报废等环节的安全要求。

8.5 人员管理

密码应用关键岗位人员应具备密码相关专业学历或专业技能认证，熟悉民用航空业务与密码技术融合要求。

8.6 建设运行

8.6.1 采购密码产品和服务时，应符合 GB/T 39204—2022 中 7.9 a)、c)、d)、g)、k)的要求。
8.6.2 应采购通过国家检测认证的网络关键设备和网络安全专用产品，形成年度采购的网络产品和服务清单，建立和维护合格供应方目录，保持网络产品和服务的稳定或多样性，明确网络产品和服务提供者的安全责任和义务。
8.6.3 应与密码服务供应方签订服务等级协议，明确职责划分和对密码服务供应方的要求，包括但不限于密码服务的连续性、安全性、合规性等方面的要求。要求其提供中文版运行维护、二次开发技术材料以及 10 年以上的知识产权的授权，对定制开发的软件进行源代码安全检测。
8.6.4 应梳理底层基础软硬件产品代码签名机制的安全风险，将风险及缓解措施纳入应急预案，当发生异常情况时，会同密码产品和服务供应方及时采取风险缓解措施，涉及重大风险的按规定向相关部门报告。
8.6.5 对密码产品和服务进行运维时，运维地点应位于中国境内，并在运维前与维护人员签订安全保密协议，不应使用未经本单位备案的运维工具。
8.6.6 供应商不应远程运维核心密码设备，确需远程运维的，应经严格授权，全程监控并留存日志，运维结束后应立即关闭远程访问通道，不应留存任何远程访问权限。
8.6.7 应根据关键信息基础设施商用密码保障系统的设计建设模式、资源供给模式，对密码产品和服务的策略配置、补丁升级等相关事项进行集中管理。

8.7 应急处置

8.7.1 应按照 GM/T 0133—2024 中 8.3 c)，根据应急预案对已发生的密码运行安全事件实施分类分级处置，并形成事件处置记录。
8.7.2 应按照 GM/T 0133—2024 中 8.3 g)，建立和完善密码运行安全事件应对知识库，包括但不限于历史安全事件经验、事件应对措施等。

8.8 安全审计

8.8.1 应采用密码技术对物理访问、网络通信、设备操作、应用交互等环节产生的日志数据进行完整性保护。
8.8.2 审计日志留存期限应不少于 1 年。

9 商用密码产品应用要求

9.1 通用要求

商用密码产品应符合合规性、可靠性、安全性、稳定性和实时性要求。附录B中列出了密码机、密钥管理类产品、身份认证类产品、综合网关类产品、工业控制专用密码产品等典型商用密码产品的核心参考性能指标。

9.2 应用要求

9.2.1 合规性要求

9.2.1.1 商用密码产品应通过商用密码产品检测认证。
9.2.1.2 网络安全等级保护第三级系统所用密码产品应符合 GB/T 37092 安全二级及以上密码模块要求。
9.2.1.3 网络安全等级保护第四级系统所用密码产品应符合 GB/T 37092 安全三级及以上密码模块要求。

9.2.2 可靠性要求

9.2.2.1 串联部署产品应支持旁路模式，硬件或软件故障时应自动切换至明文通道，切换时延不影响系统的正常运行，同时触发声光告警。不应默认启用旁路模式，启用规则应纳入应急预案，明确审计要求和回切要求。
9.2.2.2 核心产品（如密钥管理、密码机、虚拟专用网络（VPN）网关等）应支持双活热备或集群部署，切换时延不影响系统的正常运行。集群模式应支持 N+1 冗余，单节点故障不影响密码应用服务连续性。
9.2.2.3 应具备在线诊断能力和软硬件异常检测能力，异常时应自动隔离故障模块并启用备用资源，数据处理应支持断点续传。

9.2.3 安全性要求

9.2.3.1 应支持含密码技术的双因素身份鉴别，口令不少于 3 种字符类型且长度不少于 8 位，初次登录时强制要求修改，连续错误登录次数超过阈值时锁定账户。
9.2.3.2 配置策略应使用密码技术保护完整性。

9.2.4 稳定性要求

应支持固件、策略在线升级，升级时不中断业务，升级失败时回滚至前一版本。

9.2.5 实时性要求

9.2.5.1 并发处理能力、认证时延应满足民用航空业务系统的高并发业务场景密码处理能力需求。
9.2.5.2 重要业务数据端到端加密应满足业务系统对时延的要求。
9.2.5.3 支持群组广播通信的密码产品，应具备群组认证能力，满足业务系统对时延的要求。

10 商用密码应用安全性评估要求

10.1 安全性评估

10.1.1 在系统规划阶段，责任单位应分析系统面临的安全风险和风险控制需求，明确商用密码应用需求，编制商用密码应用方案，委托商用密码应用安全性评估机构对方案进行评估，评估通过后方可实施。
10.1.2 在系统建设阶段，责任单位应按照商用密码应用方案建设密码保障措施，建设完成后，委托商用密码应用安全性评估机构对商用密码应用建设情况进行评估，评估通过后系统方可上线运行。
10.1.3 在系统运行阶段，责任单位应每年对系统开展商用密码应用安全性评估，与网络安全等级保护测评、关键信息基础设施安全评估相衔接。
10.1.4 系统如发生重大变更（如系统架构重大变化等）或发生涉及密码应用的安全事件，应在变更完成或事件处置后 3 个月内重新开展商用密码应用安全性评估。
10.1.5 责任单位在商用密码应用安全性评估报告形成后 30 日内，应将评估报告和相关工作情况按照国家和行业主管部门有关要求报送国家密码管理局或属地密码管理部门备案，同时报送行业主管部门。

10.2 评估整改

10.2.1 责任单位应针对未通过商用密码应用安全性评估的系统，根据存在问题制定整改方案并进行整改，消除安全风险。
10.2.2 责任单位应在商用密码应用安全性评估报告出具后 30 日内制定整改方案，及时进行整改。
10.2.3 整改完成后，责任单位应开展整改情况复核，如未通过复核继续整改，针对确难整改的采取风险缓解措施，直至通过商用密码应用安全性评估。

附 录 A
（资料性）
商用密码应用保护对象和应用场景

民用航空重要网络与信息系统中商用密码应用保护对象和应用场景见表A.1。

表 A.1 商用密码应用保护对象和应用场景

网络与信息系统类型	机密性技术要求保护对象	完整性技术要求保护对象	真实性技术要求应用场景	不可否认性技术要求保护对象
空中交通管理类信息系统	气象探测原始数据（如雷达基数据、自观原始数据等），达到一定精度的地理空间信息数据，未公开的空域数据等	空管自动化系统的监视数据，空中交通服务电报（如动态和管制电报、飞行情报电报、气象情报电报等），民航气象信息共享与服务系统的气象数据，达到一定精度的地理空间信息数据，未公开的空域数据等	空管自动化系统的监视源通信实体身份（如ADS-B地面站、雷达站等），全国流量系统的航班放行时隙、流量管理措施发布者身份，民用航空气象信息共享与服务系统数据发布者身份，航空情报自动化系统的航行通告数据发布者身份等	空中交通服务电报（如动态和管制电报、飞行情报电报、气象情报电报等）拍发及承转记录，全国流量系统的航班放行时隙、流量管理措施发布记录，航空情报原始资料更新审批发布记录，相关系统对航空情报数据的更新记录等
航空器运行保障类信息系统	航班运行控制系统的起降时刻、航线参数、备降机场等飞行计划数据，飞行员网上准备系统的发动机状态、燃油容量等飞机参数，机务维修管理系统的飞机维修记录、部件寿命等飞机适航数据等	航班运行控制系统的起降时刻、航线参数、备降机场等飞行计划数据，飞行员网上准备系统的发动机状态、燃油容量等飞机参数，机务维修管理系统的飞机维修记录、部件更换、部件寿命等飞机适航数据，航材管理系统的航材库存变动、出入库等记录，系统用户身份鉴别、操作行为日志数据，其他重要业务数据等	航班运行控制系统的航班调整信息发布者身份，地面保障系统的保障进度数据发布者身份，飞行员网上准备系统的飞行员身份，机务维修管理系统的维修人员身份，航材管理系统的航材出入库操作发起者身份等	航班运行控制系统的航班延误/取消、航线变更等调整审批记录，地面保障系统的加油完成、除冰达标等保障确认记录，飞行员网上准备系统的飞机参数确认操作记录，机务维修管理系统的飞机维修合格验收、部件更换审批记录，航材管理系统的航材入库检验、出库领用确认记录等
航空服务类信息系统	常旅客管理系统的会员数据等商业秘密，离港控制系统的值机数据等业务数据，旅客证件号、联系方式、支付账号等个人敏感信息，系统用户身份鉴别数据，其他重要业务数据等	常旅客管理系统的会员积分变动数据等商业秘密，电子客票系统的客票信息变更记录，离港控制系统的值机操作记录等业务数据，旅客证件号、联系方式、支付账号等个人敏感信息，系统用户身份鉴别、操作日志数据，其他重要业务数据等	航空公司、代理人、机场用户在订座、出票、离港环节登录对应系统的用户身份，个人值机、机票改签、商城消费等操作发起者身份，离港前端系统的值机操作终端身份等	电子客票系统的客票出票、退改记录，电子行程单开具记录等，离港控制系统的值机操作、座位调整等操作记录，常旅客管理系统的会员积分变动、等级调整审批记录等

表A.1　商用密码应用保护对象和应用场景（续）

网络与信息系统类型	机密性技术要求保护对象	完整性技术要求保护对象	真实性技术要求应用场景	不可否认性技术要求保护对象
机场生产运行类信息系统	信息集成系统的航班起降时刻、航路航线、任务性质等飞行计划数据，机场资源能力、资源分配等协同决策数据，离港前端系统的旅客姓名、证件号、联系方式等个人敏感信息，旅客值机状态、座位号、托运行李等值机数据等	信息集成系统的航班起降时刻、航路航线、任务性质等飞行计划数据，航班动态、航班保障节点等航班运行数据，机场资源能力、资源分配等协同决策数据，离港前端系统的旅客姓名、证件号、联系方式等个人敏感信息，旅客值机状态、座位号、托运行李等值机数据等	信息集成系统的航班计划发布者、航班状态变更者、航班资源分配者的身份等	信息集成系统的航班计划发布记录、航班状态变更记录、航班资源分配记录、航班保障记录，离港前端系统的旅客值机记录、行李托运记录等
航空安全保卫类信息系统	安全检查信息管理系统的旅客姓名、证件号、联系方式、人脸图像等旅客数据等	安全检查信息管理系统的旅客姓名、证件号、联系方式、人脸图像等旅客数据，旅客安检状态、过检时间等安检数据等	安检信息管理系统的安检人员身份等	安全检查信息管理系统的旅客过检记录等
行业监管与企业安全管理类信息系统	航班时刻管理系统的航班起降时刻、任务性质等飞行计划数据，民用航空飞行标准监督管理系统的行政许可批复等敏感政务数据等	航班时刻管理系统的航班起降时刻、任务性质等飞行计划数据，民用航空飞行标准监督管理系统的飞行员执照审批等行政许可批复政务数据等	民用航空飞行标准监督管理系统的行政许可审批人员身份，航班时刻管理系统的航班时刻发布者、审批者的身份信息，适航审定运行管理系统的适航数据发布者身份等	民用航空综合统计信息系统的行业统计数据报送、发布审批记录，民用航空飞行标准监督管理系统的飞行员执照审批、行政许可批复记录，政务公文签发、流转确认记录，航班时刻管理系统的航班计划变更记录等
公共信息服务类信息系统	门户网站的后台管理账户、密码、会话ID等凭证数据	门户网站的后台管理账户、密码、会话ID等凭证数据等	门户网站的后台管理者身份等	门户网站的信息发布记录等
基础支撑类设施平台	民航云计算平台的租户数据，大数据平台内多种数据关联、合并后的数据，旅客行为分析数据，核心网络的路由配置数据等	民航云计算平台的租户数据，大数据平台内多种数据关联、合并后的数据，旅客行为分析数据，核心网络的路由配置数据等	民航云计算平台的租户身份，大数据平台数据交互API接口，核心网络的访客等实体身份	民航云计算平台的租户资源分配、权限变更审批记录，大数据平台的数据操作、数据发布、数据流转记录，核心网络的配置变更记录等
其他信息设施	工业控制设备（PLC控制器、RTU）配置参数，服务器、工业控制主机操作系统敏感配置信息，重要可执行程序（核心固件）的核心代码片段，油库供油（长输管道）自动化系统的管道压力、油罐液位等作业调度数据等	工业控制设备（PLC控制器、RTU）配置参数，服务器、工业控制主机操作系统敏感配置信息，重要可执行程序（核心固件）的核心代码片段，油库供油（长输管道）自动化系统的管道压力、油罐液位等作业调度数据等	PLC控制器、RTU等工业控制设备身份，服务器、工业控制主机的可信平台身份，重要可执行程序（如核心固件）来源，航油加注调度作业人员身份等	工业控制设备的程序下载、参数配置变更记录，工业控制设备程序更新操作记录，油库供油（长输管道）自动化系统的加油调度作业记录等

附 录 B
（资料性）
典型商用密码产品核心性能

B.1 密码机

B.1.1 用途

密码机是用于数据加密传输、存储的核心设备，适配民用航空通用、高并发、低时延和工业控制等业务场景。

B.1.2 核心性能指标

B.1.2.1 通用场景

支持双活热备，切换不超过60 s。非对称加解密并发量不少于二千次每秒，签名并发量不少于二千次每秒。对称加密性能不少于200 Mbps。

注：通用场景包括电子政务系统、通用管理系统等。

B.1.2.2 高并发场景

采用集群部署（如3+1集群），切换不超过10 s。支持负载均衡与弹性扩容。SM2非对称加解密并发量不少于每秒十万次，SM2签名并发量不少于每秒十万次。对称加密性能不少于5 Gbps。

注：高并发场景包括旅客服务、离港系统等。

B.1.2.3 低时延场景

采用双活并支持异地灾备，切换不超过20 ms。非对称加解密并发量不少于每秒一万次，签名并发量不少于每秒一万次。对称加密性能不少于1 Gbps。

注：低时延场景包括空管系统等。

B.1.2.4 工业控制场景

采用双活并支持旁路模式，切换不超过40 ms。支持Modbus、OPC UA等工业协议。非对称加解密并发量不少于每秒五千次，签名并发量不少于每秒五千次。对称加密性能不少于200 Mbps。

注：工业控制场景包括助航灯光、油库系统等。

B.2 密钥管理类产品

B.2.1 用途

密钥管理类产品用于密钥全生命周期管理，适配高可用、低延迟业务场景。

B.2.2 核心性能指标

支持两地三中心部署（主数据中心、本地灾备中心、异地实时灾备中心），密钥同步时延不超过100 ms，单中心故障时备用中心接管时间不超过30 s。

非对称密钥生成响应时间不超过50 ms，对称密钥生成响应时间不超过30 ms，密钥分发时间不超过100 ms。

支持SM2、SM3、SM4、SM9等密码算法。

B.3 身份认证类产品

B.3.1 用途

身份认证类产品用于用户和设备的身份鉴别，适配高并发与强绑定业务场景。

B.3.2 核心性能指标

支持双活热备，证书签发切换时间不超过30 s，证书吊销列表（CRL）更新时间不超过1 h。双因子终端（如USBKey、移动设备）应支持离线认证，适配无网络场景。

旅客场景的并发认证性能不低于每秒十万次（如线上值机等），运维场景的并发认证性能不低于每秒一万次，设备认证的并发认证性能不低于每秒五千次。

支持SM2、SM3、SM4、SM9等商用密码算法，终端鉴别支持动态令牌、USBKey等方式。

B.4 综合网关类产品

B.4.1 用途

综合网关用于网络与通信安全、设备与计算安全环节中通信实体的身份鉴别、通信数据的机密性和完整性保护。

B.4.2 核心性能指标

支持双活热备，切换不超过60 s，SSL加密吞吐不少于1 Gbps，隧道密文速率不少于1 Gbps。

支持IPv6转IPv4、IPv4转IPv6。

支持同一个端口同时自适应RSA证书与SM2证书。

支持互联网安全协议（IPSec）协议和SSL协议。

B.5 工业控制专用密码产品

B.5.1 用途

工业控制专用密码产品适配机场运维类工业控制场景，支持工业协议与恶劣环境业务场景需求。

注：工业控制专用密码产品包括PLC模块、工控防火墙等。

B.5.2 核心性能指标

支持双活与旁路模式，PLC模块故障不影响控制功能，切换时间不超过30 ms。耐受-40 ℃～70 ℃温度、5%～95%湿度（无冷凝），适配户外、油库等场景。

工业协议解析时间不超过20 ms，支持Modbus、OPC UA、DNP3等协议，加密指令处理性能不小于每秒一百条。单模块最大接入工业控制设备不少于100个。

支持SM2、SM3、SM4、SM9等商用密码算法。

参 考 文 献

[1] GB/T 5271.8—2001 信息技术 词汇 第8部分：安全
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 28448—2019 信息安全技术网络安全等级保护测评要求
[4] GB/T 32905—2016 信息安全技术 SM3密码杂凑算法
[5] GB/T 32907—2016 信息安全技术 SM4分组密码算法
[6] GB/T 32918 信息安全技术 SM2椭圆曲线公钥密码算法
[7] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
[8] GB/T 43206—2023 信息安全技术 信息系统密码应用测评要求
[9] GB/T 43207—2023 信息安全技术 信息系统密码应用设计指南
[10] GM/T 0022—2023 IPSec VPN技术规范
[11] GM/T 0024—2023 SSL VPN技术规范
[12] GM/T 0119—2022 PLC控制系统及PLC控制器密码应用技术规范
[13] GM/Z 4001—2013 密码术语
[14] MH/T 0051—2015 民用航空信息系统安全等级保护实施指南
[15] MH/T 0069—2018 民用航空网络安全等级保护定级指南
[16] MH/T 0076—2020 民用航空网络安全等级保护基本要求
[17] MH/T 3039—2025 民航领域数据分类分级要求